GESTION DES CRISES
Pour un vocabulaire de crise raisonné et partagé

Alain Dequier

Risk manager
Secrétariat général
Commission bancaire

Pierre Poulain

Chargé de mission auprès du Contrôleur général pour la Prévention des risques
Banque de France

Avec la contribution des membres de la profession bancaire.

En septembre 2004, Banque magazine* contenait un article sur le vocabulaire de crise qui ne pouvait présenter tous les termes. Aussi, il nous a paru souhaitable de passer en revue les plus fréquents et d'indiquer pourquoi nous avons pu leur préférer un équivalent.

Dans le domaine des « plans », quatre expressions fréquentes n'avaient pas été évoquées.

D'abord la traduction de l'expression « *contingency planning* », très répandue dans les textes anglo-saxons. « *Contingency* » évoque des événements non prévus, incertains. Cette référence à l'incertitude correspond bien à des situations jamais vécues jusqu'à présent, comme ce fut le cas pour le passage à l'an 2000, ou aujourd'hui pour certaines questions environnementales ou médicales. Aucun équivalent en français ne s'impose. Il est donc préférable de parler uniquement de plan de continuité d'activité (PCA), plan bien défini par son objectif clairement énoncé.

Le plan de contournement est aussi très employé, il s'agit plutôt de moyens de contournement (« *workaround solution* »). Contournement est synonyme d'évitement, il peut être vu comme une astuce pour éviter un problème, pour ne pas réellement se le poser (qui donnerait « *to bypass* ») mais, de fait, le terme est retenu pour des solutions transitoires à l'intérieur d'un plan de secours permettant de poursuivre les opérations et activités prioritaires [1].

Un sigle est très connu des établissements de crédit : le PSI, le plan de secours informatique. Il n'était pas mentionné dans l'article de septembre. Ce terme est utilisé de longue date ; bien avant que ne se généralise l'exigence de PCA, les directions informatiques ont augmenté la qualité de leurs propres prestations. Les PSI répondent à l'objectif de disponibilité [2] des ressources informatiques. Ils constituent souvent une partie importante des PCA mais jamais leur totalité, les « lignes de métiers » doivent envisager des cas plus graves, plus perturbants, que le seul arrêt du centre informatique principal.

> *« Les établissements doivent anticiper la couverture des postes prioritaires ainsi que la redistribution des responsabilités en cas de crise et en assurer le maintien opérationnel. »*

Des plans de substitution peuvent être élaborés pour traiter une partie des questions relatives aux ressources humaines. Les chocs extrêmes (« *extreme event* » ou « *major disruption* »), face auxquels le règlement CRBF 2004-02 demande d'être robuste, englobent des cas d'indisponibilités de ressources humaines. Les établissements doivent donc anticiper la couverture des postes prioritaires, ainsi que la redistribution des responsabilités en cas de crise, et en assurer le maintien opérationnel. Cette mesure étend le champ d'application de la recommandation du livre blanc de la Commission bancaire sur la sécurité des systèmes d'information relative aux hommes clés (« *key-persons* »), rendus indispensables. Une gestion des ressources humaines, compatible avec la continuité d'activité, suppose donc de placer en haute priorité la polyvalence des agents et leur substituabilité pour faire la chasse aux situations que l'on pourrait qualifier de « *single man failure* » (par analogie à l'expression anglo-saxonne « *single point of failure* » c'est-à-dire qu'il existe un point qui, s'il est détruit et faute de redondance, provoque une défaillance totale). Sur ce thème, pour assurer la robustesse par la redondance, il est possible soit de répartir les compétences dans des unités géographiquement éloignées, soit de faire appel à des réservistes, personnel addition-

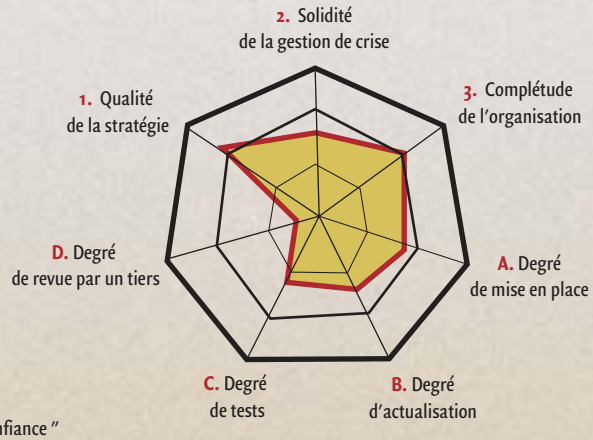
* Banque magazine, n° 661, septembre 2004, p. 50-52.

EXEMPLE D'UN OUTIL D'ÉVALUATION DES PCA

La Banque de France a développé un questionnaire évaluant le niveau de préparation de ses différents métiers les plus sensibles en matière de Plan de continuité d'activités.

Les thèmes couverts sont :
1. La qualité de la stratégie de continuité (nombre de scénarios couverts, niveau de poursuite de l'activité…),
2. L'aptitude à mobiliser toutes les ressources utiles dès le début de la crise et à les piloter ensuite,
3. La prise en compte de toutes les composantes d'un PCA (secours, reprise, tests…).

Données fictives



En outre, le traitement des réponses permet de dégager quatre " indicateurs de confiance " dans la capacité de ces PCA à faire réellement face à un choc extrême :
A) Le degré de mise en place (ou l'éloignement des échéances pour le reste à faire),
B) Le degré d'actualisation des différentes composantes,
C) Le caractère éprouvé ou non du PCA, en fonction du caractère plus ou moins complet et représentatif des tests,
D) La garantie supplémentaire que peut apporter une revue par un tiers.

nel appelable en renfort pour son expérience des activités.

LES DEUX APPROCHES DU PCA

À propos des scénarios que le plan de continuité doit prendre en compte, deux approches sont possibles, selon les causes ou les impacts. Imaginer des causes d'incidents ou de catastrophes est une activité sans fin. Mais rapidement on peut constater que les impacts correspondants ont des conséquences identiques : les disparitions de locaux, de systèmes d'information ou de production, voire de ressources humaines. Le RPCA, responsable des PCA, se concentrera sur les différents cas d'indisponibilités de ressources, qu'on appellera scénarios d'impact qui sont en nombre réduit. Le *risk manager* (RM) de son côté, analysera les causes, origines possibles des indisponibilités, dans une optique de réduction de la vulnérabilité de l'entreprise. À ce propos, notons que l'expression anglaise *risk manager* s'impose aujourd'hui pour la fonction, ses traductions françaises peuvent être gestionnaire des risques (GR), ou mieux, responsable de la prévention – ou de la maîtrise – des risques (RPR/RMR) [**3**].

LES AUTRES TERMES

Le schéma présentant la chronologie de la crise dans l'article de septembre ne mentionnait pas les actions de communication interne et externe, cette question pourrait alimenter un article à elle seule, en particulier sur le dilemme qui consiste à, simultanément, satisfaire les médias, maintenir l'image de l'entreprise et ne pas perturber les opérations en cours.

De même, la question des tests a seulement été évoquée parmi les missions du RPCA. Celle-ci est à développer puisque les tests se déclinent selon les domaines (techniques, fonctionnels), leur périmètre (local, global, de Place) ou leur profondeur (simulation, répétition (« *dry run* »), *crash test* [**4**]). Ils doivent être accompagnés d'un contrôle pour s'assurer de la cohérence d'ensemble des PCA. L'évocation de la reconstitution des données (« *data recovery* ») avec la resynchronisation de traitement pouvait laisser penser que les données n'avaient pas de problèmes de synchronisation. La reconstitution doit bien englober :

- les données perdues entre la dernière sauvegarde et le crash, à reconstituer manuellement ;
- les données reçues mais non traitées, à réintroduire ultérieurement dans les traitements ;
- les données générées par les activités maintenues, à réintroduire dans le système reconstruit.

À propos de la mallette de crise (« *crisis battle box* »), il faut distinguer, d'une part, les équipements pour piloter la crise, destinés aux membres de la cellule de crise, et d'autre part, les informations à détenir sur soi pour réagir au déclenchement de la crise. Pour le plus grand nombre, ces informations se réduiront à quelques consignes. Le terme mallette de crise ne recouvre pas toute la documentation des PCA.

Enfin, à la question toute simple « Comment désigner la solution mise en place pour assurer la continuité de l'activité ? », il convient d'être prudent, de retenir pour réponse le mot plan et non « solution de continuité », car cette expression, usitée dans le monde médical pour désigner une fracture, désignerait la rupture, la disparition de la continuité, tout comme la solution d'un problème peut être interprétée comme ce qui fait disparaître le problème. L'expression « solution pour la continuité » serait acceptable, mais un peu lourde, d'où la préférence pour plan de continuité. ■

[1] Les activités peuvent être classées selon leur sensibilité en vitale, stratégique, critique ou sensible.
[2] Les autres facteurs sont l'intégrité, la confidentialité et la possibilité de preuve, résumés en DICP.
[3] On pourrait aussi promouvoir le terme responsable de la mitigation des risques qui ferait écho à l'activité de « *risk mitigation* » des anglo-saxons, en nous restituant le vieux mot français, mitigation, un peu plus oublié.
[4] *Simulation* et *crash test* se diraient de même en anglais, à la réserve près que pour le second terme les anglophones penseraient plus à un test surprise qu'à un test des hypothèses extrêmes.